CPS-Small: Energy-Aware Formal Synthesis for Supervisory Control and Information Acquisition in Cyber-Physical Systems

Stéphane Lafortune, University of Michigan

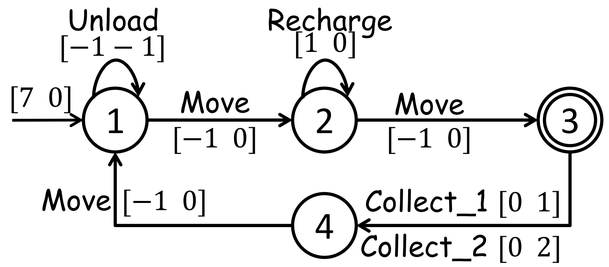
https://wiki.eecs.umich.edu/stephane/index.php/CPS_Energy

CPS-PI Annual meeting, June 3-4, 2021

Project period: 10/2017-09/2021

Objective

Investigate theoretical foundations and develop computational algorithms to synthesize higher-level formal control and information acquisition logic in cyber-physical systems that satisfy *both qualitative* and *quantitative* requirements.



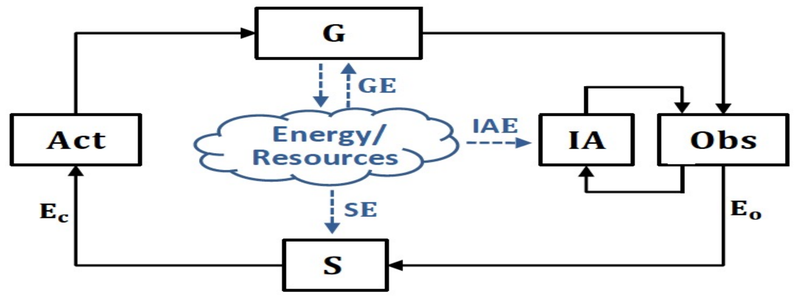
A simple energy-aware robot mission planning example with two types of resources: battery energy and amount of trash. The initial energy is [7 0].

Achievements (Cumulative)

- Optimal supervisory control scheme to regulate the rate of resource consumption/renewal under limited sensing capabilities
- Interface-based approach for security obfuscation under qualitative and quantitative constraints
- Novel synthesis techniques for supervisors that are robust to sensor deception attacks

- **Graduate Students at Michigan**: Yiding Ji, Rômulo Meira Góes, Andrew Wintenberg
- **Collaborators**: Blake Rawlings (Sandia National Laboratories); Sahar Mohajerani (Chalmers U.; Xiang Yin (Shanghai Jiao Tong U.)

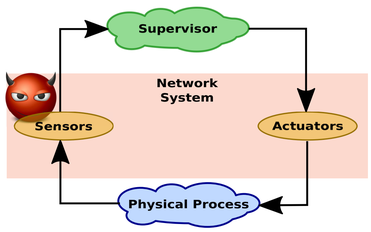
Energy-Aware Control with Imperfect Information



Energy-Aware Supervisory Control and Information Acquisition System

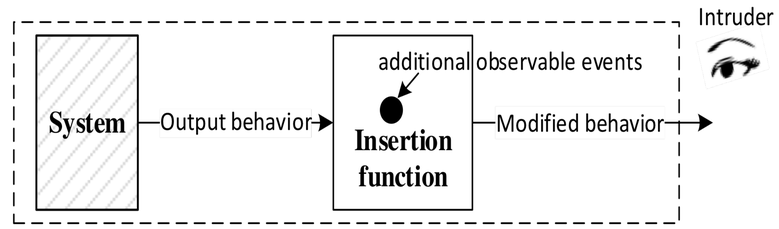
- Control strategy regulates resource flows so that the system's resource level or long run average rate remains above certain threshold
- Optimal supervisor is designed to optimize the long run average flow rate
- A two-player quantitative game structure is constructed to encode supervisors
- A min-max game is solved to synthesize supervisors for the optimal control problem

Robustness to Sensor Deception Attacks



- Add potential Sensor Deception attacks in the supervisor synthesis algorithms

Energy-Constrained Obfuscation for Secrecy



- Intruder: malicious outside observer that infers system secrets from its observations
- Opacity: plausible deniability to preserve secrets from the intruder's inference
- Defender: inserts fictitious events at the output of the system to obfuscate the intruder and preserve system secrets (qualitative constraints)
- The defender's strategies are constrained by the *resource capacities* of the system, i.e., there are *quantitative* constraints on insertion functions
- General solution methodology developed based on formal methods and graph games.

Selected Publications

- Y,Ji, X. Yin and S. Lafortune. Enforcing Opacity by Insertion Functions under Multiple Energy Constraints, Automatica, October 2019.
- S.Mohajerani, Y. Ji, and S. Lafortune, "Compositional and Abstraction-Based Approach for Synthesis of Edit Functions for Opacity Enforcement." IEEE TAC, August 2020.
- Y,Ji, X. Yin and S. Lafortune. Optimal Supervisory Control with Mean Payoff Objectives and under Partial Observation, Automatica, In Print.
- R. Meira-Góes, H. Marchand, and S. Lafortune, "Synthesis of Supervisors Robust Against Sensor Deception Attacks," IEEE TAC. In print.

Award ID#: CNS-1738103